

Carbanak Group uses Google for malware command-and-control

 forcepoint.com/blog/x-labs/carbanak-group-uses-google-malware-command-and-control

January 17, 2017

X-Labs

January 17, 2017

Nicholas Griffin Security Researcher

Google Malware

Forcepoint Security Labs™ recently investigated a trojanized RTF document which we tied to the Carbanak criminal gang. The document contains an encoded Visual Basic Script (VBScript) typical of previous Carbanak malware. Recent samples of the malware have now included the ability to use Google services for command-and-control (C&C) communication. We have notified Google of the abuse and are working with them to share additional information.

Carbanak (also known as Anunak) are a group of financially motivated criminals first exposed in 2015. The actors typically steal from financial institutions using targeted malware. Recently a new Carbanak attack campaign dubbed "Digital Plagiarist" was exposed where the group used weaponized office documents hosted on mirrored domains, in order to distribute malware.

Weaponized document

The RTF document we analyzed (SHA1 *1ec48e5c0b88f4f850facc718bbdec9200e4bd2d*) has an embedded OLE object which contains a VBScript file. When the document is opened the targeted user is lured into double-clicking on the embedded OLE object which is disguised as an image:

PROTECTED DOCUMENT

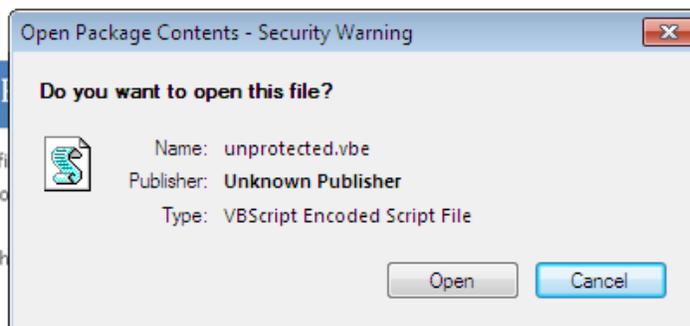
This document is protected by Microsoft Office and requires human verification. Please Enable Editing and Double Click below to prove that you are not a robot.



Double Click Here
To Unlock Contents

CAN'T VIEW?

1. Open the document in Microsoft Office.
2. If you downloaded this document from the internet, click the "Enable Editing" button above.
3. Double click above. The content of the document will be unlocked.



Double clicking on the image results in a file open dialog for "unprotected.vbe". If the user executes this file then the VBScript malware will begin to execute.

Encoded VBScript malware

The VBScript malware inside the RTF document (SHA1 *cd75662751c59951717b4704ea2cdb6fb7ec19bc*) is an encoded VBScript file. We decoded the script and found hallmarks typical of the Carbanak group's VBScript malware, however we also found the addition of a new "gglldr" script module.

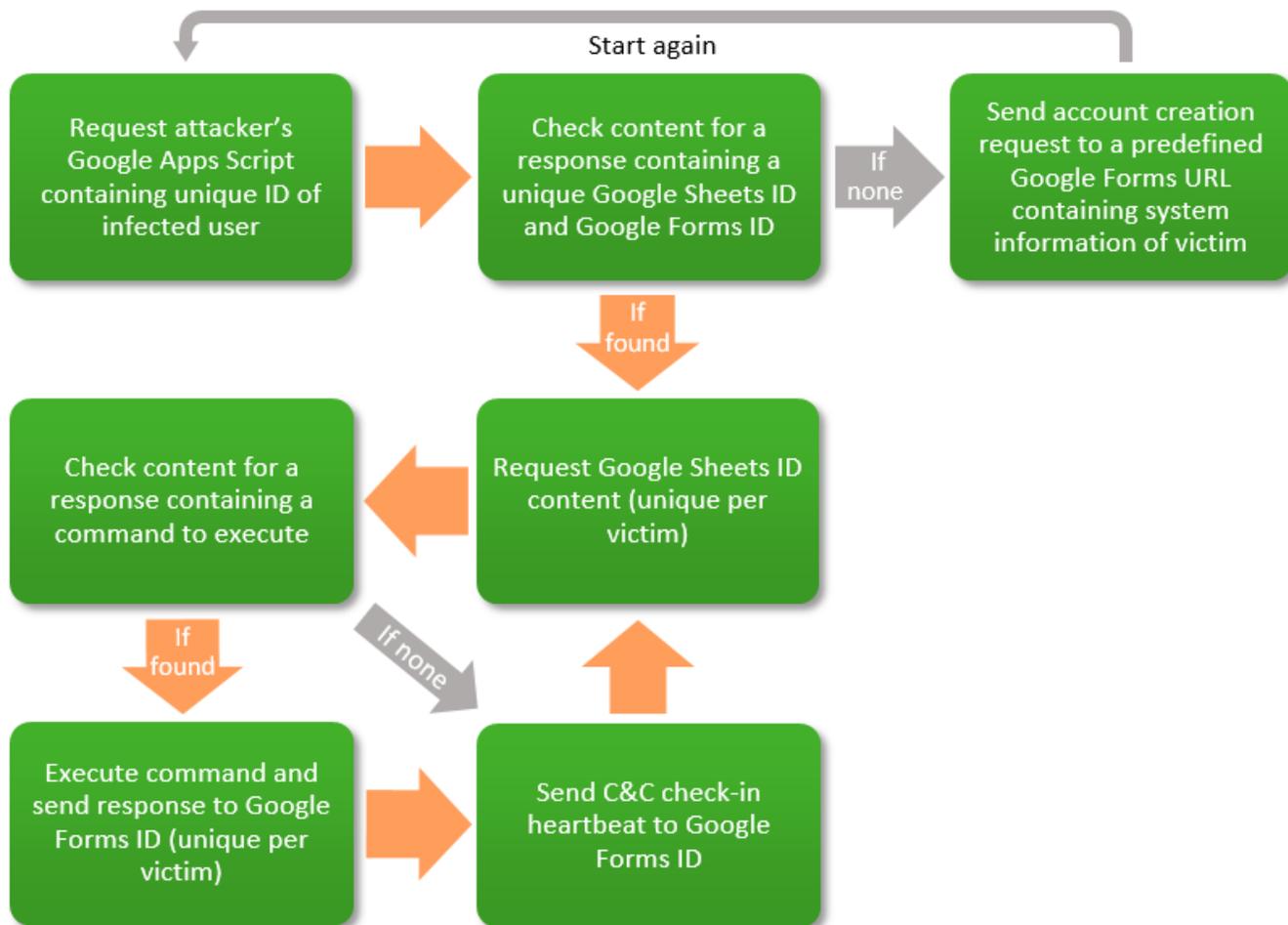
```
dIm box
box="RFFwY1RHRnpkRU50Wk2ObFkzUnBiMjVkrFFwc11YTjBYMk50WkY5cFpEMHhEUW9OQ2x0U2RXNVRaV04wY...
dIm gGldr
gglldr="T24gRXJyb3IgaUmVzdW11IE5leHQNCmRpbSB1eGVjRmlsZU5hbWUsIHN0YXJ0RmlsZU5hbWUNCmV4ZWN...
```

The module is base64 encoded inside the main VBScript file along with various other VBScript modules used by the malware. When we analyzed the script we noticed that it is capable of using Google services as a C&C channel.

Abusing Google for C&C communication

The "gglldr" script will send and receive commands to and from Google Apps Script, Google Sheets, and Google Forms services. For each infected user a unique Google Sheets spreadsheet is dynamically created in order to manage each victim. The use of a legitimate third party service like this one gives the attacker the ability to hide in plain sight. It is unlikely that these hosted Google services are blocked by default in an organization, so it is more likely that the attacker will establish a C&C channel successfully.

The C&C procedure is outlined in the diagram below.



Upon the first attempt to contact the hard-coded Google Apps Script URL with the user's unique infection ID, the C&C will state that no spreadsheet currently exists for the user. The malware will then send two requests to another hard-coded Google Forms URL which will result in the creation of unique Google Sheets spreadsheet and Google Form IDs for the victim.

The second time the Google Apps Script is requested, the C&C will return the unique Google Sheet and Google Form ID values:

```

x22,\x22userHtml\x22:\x22:\x22
x22\1yPpEGSRsu0PuPqj1B4NE4XOYvcsXRSyOMEFH1bH oM$$$
17oZer_3Wm7JDtDcx2Hp58FMfhOc85AeydQQjNs_3F6E$$$entry-
1548304398\x22,\x22ncc\x22:\x22{\x22awhs\x22:true
  
```

- spreadsheetkey
- formkey
- entry

The "entry" value is also a unique ID which is sent with each subsequent Google Forms C&C request.

Protection statement

Forcepoint™ customers are protected against this threat via TRITON® ACE at the following stages of attack:

Stage 5 (Dropper File) - The malware components are prevented from being downloaded and/or executed.

Stage 6 (Call Home) - The HTTP-based Carbanak C&C traffic is blocked.

Summary

The Carbanak actors continue to look for stealth techniques to evade detection. Using Google as an independent C&C channel is likely to be more successful than using newly created domains or domains with no reputation. Forcepoint will continue to monitor this group's activities and share data with trusted partners.

Indicators of Compromise

Carbanak Documents

1ec48e5c0b88f4f850facc718bbdec9200e4bd2d (3-ThompsonDan.rtf)
400f02249ba29a19ad261373e6ff3488646e95fb (order.docx)
88f9bf3d6e767f1d324632b998051f4730f011c3 (claim.rtf)

Carbanak Google Apps Script C&Cs

hxxps://script.google[.]com/macros/s/AKfycbzuykcvX7j3TlBNyQfxtB1mqii31b4VT0N640yiRJT0t6rS4s4/exec
hxxps://script.google[.]com/macros/s/AKfycbxxx5DHR0F8AYhLuDjnp7kGNELq6g27J4c_JWwx1p1nDfZh6In0/exec
hxxps://script.google[.]com/macros/s/AKfycbwZHCgg5EsCiPup_mNxDbSX7k7yBMeXWen0VN1BWXHmyBpb8ng/exec

Carbanak Google Forms C&Cs

hxxps://docs.google[.]com/forms/d/e/1FAIpQLScx9gwNadC7Vjo11mXLbU3aBQRrqVpowjmnNJ1ZneqpjaYLE3g/formResponse
hxxps://docs.google[.]com/forms/d/e/1FAIpQLSfE9kshYBFSDAfrClw8m9rAdajqoYhzhEYmEAgZexE3LQ-17A/formResponse
hxxps://docs.google[.]com/forms/d/e/1FAIpQLSdcdE7lTEiqV5MW3Up8Hgy5NGkIKnLKoe0YPFriD4_9qYq9A/formResponse

Carbanak C&Cs

hxxp://atlantis-bahamas[.]com/css/informs.jsp
hxxp://138[.]201[.]44[.]4/informs.jsp

Carbanak Cobalt Strike / Meterpreter DNS Beacon C&Cs

aaa.stage.15594901.en.onokder[.
]com
aaa.stage.4710846.ns3.kiposerd[.
]com

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

[Learn more about Forcepoint](#)